A Support Middleware Solution for e-Healthcare System Security

Ndibanje Bruce*, Mangal Sain**, Hoon Jae Lee**

*Department of Ubiquitous IT, Graduate School of Dongseo University, Sasang-Gu, Busan 617-716, Korea

** Division of Computer and Engineering Dongseo University Sasang-Gu, Busan 617-716, Korea

ndibanje.bruce.phd@ieee.org, mangalsain1@gmail.com,hjlee@dongseo.ac.kr

***Abstract*— This paper presents a middleware solution to secure data and network in the e-healthcare system. The e-Healthcare Systems are a primary concern due to the easiest deployment area accessibility of the sensor devices. Furthermore, they are often interacting closely in cooperation with the physical environment and the surrounding people, where such exposure increases security vulnerabilities in cases of improperly managed security of the information sharing among different healthcare organizations. Hence, healthcare-specific security standards such as authentication, data integrity, system security and internet security are used to ensure security and privacy of patients' information. This paper discusses security threats on e-Healthcare Systems where an attacker can access both data and network using masquerade attack. Moreover, an efficient and cost effective approach middleware solution is discussed for the delivery of secure services.**

***Keywords*— e-Healthcare; Middleware; Data Security; Network Security;**

I. INTRODUCTION

The recent advances in Information and Communication Technology domain have given rise to many networks and application as well. The efforts done by different researchers have produced huge and beneficial technologies, devices, and services adhering to them. Those devices are typically designed for specific tasks such as sensing, data processing and communication purposes. With this regards, security is primary concern to ensure the whole communication between the devices passing through networks systems

Following the problem statement, many novel challenges ore offered by the growth of the application's wireless healthcare offers, like, reliable data transmission, node mobility support and fast event detection, timely delivery of data, power management, node computation and middleware [1-3]. In addition through, deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable. For instance, the patient's physiological vital signals are very sensitive (*i.e.*, if a patient has some embarrassing disease), so any leakage of individual disease data could makes him/her embarrassed. In fact sometimes revealing disease information can result in a person losing his/her job, or make it impossible for him/her to obtain insurance protection.

The latter trend marks an ever-growing and clamant need for protecting the confidentiality and integrity of health-care information, whilst at the same time ensuring its availability to authorized health-care providers. However, one has to acknowledge the fact that complete protection of data is, in practice, neither feasible nor possible.

This paper deals with data and network attacks on healthcare system by masquerade attack and we describe a countermeasure protocol based against this attack. The remainder of this paper is organized as follows: Section 2 present related work while Section 3 describes the attack overview on the e-healthcare system. Section 4 present the proposed middleware solution and Security analysis is done in section 5. Finally Section 6 concludes the paper.

.

II. RELATED WORK

For the trustworthy of data and network security of the e-Healthcare systems, a large number of protections techniques have been addressed. In the following, we provide an overview of some existing security implementations for e-Healthcare systems.

A solution to unsure the communication among wireless sensor network to support e-Healthcare systems has been proposed in [4]. A classification level based has described where the information among the system is leveled from level 5 to level 1. Level 5 is the data which do not comprise any sensitive information and allow public access. Along with the security level increases, to access the data becomes more and more critical. For the data marked as level 1, they are extremely sensitive and only allow few people to access. Different users are assigned to a predefined level. If the users involved in the communication belong to the same level, the communication is at the same level. If the users involved in the communication do not belong to the same level, the communication will be happened at the lower value level. When the communication level is determined, different strength encryption algorithms are applied to the communication using keys from 80 bits up to 192 bit or longer. To provide security for online systems (PCASSO), a scheme based implementation of patient centered access has

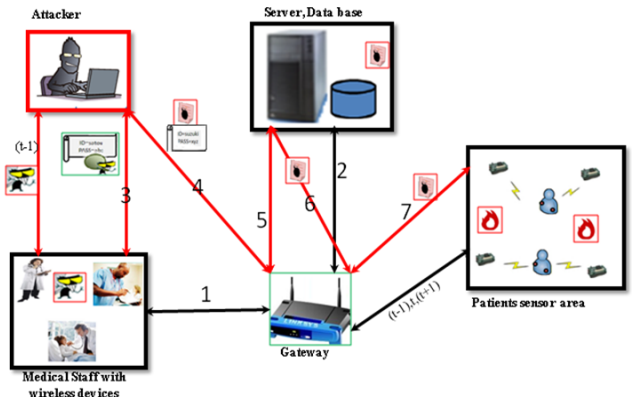

Figure 1. Masquerade attack overview

been proposed by Masys et al. [5]. Initially, it aims to permit patients and health care providers to access health information, even the sensitive data. Their access scheme combines role-based access control, mandatory access control and discretionary access control. The implementation is a patient-centered and centralized approach that stores all the data on a single server.

III. Masquerade Attack Description On e-Healthcare System

In general, a masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism.

In generally, the attempt may come from within the hospital, for example, from a medical staff; or from an outside user through some connection to the public network. Weak authentication provides one of the easiest points of entry for a masquerade, since it makes it much easier for an attacker to gain access. Once the attacker has been authorized for entry, they may have full access to the patient's critical data, and (depending on the privilege level they pretend to have) may be able to modify and delete patients 'records from the data base, make changes to network configuration and routing information.

Moreover, in any e- Healthcare Wireless Sensor Network, a masquerade node can apply easily denial-of-service attacks, and can disrupt the application operation. It can even defeat the purpose of wireless healthcare. Thus, masquerading nodes can be very dangerous for healthcare applications. More important, if a masquerade relay node captures the patient physiological data, later, these captured messages can pose replay threats to the real-time healthcare application. Obviously, the patient treatment depends on fresh received messages from medical sensor networks. If masquerade nodes replay the old messages again and again, this could cause of mistreatment and overtreatment (i.e., medicine overdose) of the patients. Thus, masquerade and replay threats endanger real-time healthcare applications using wireless medical sensors. Figure1 shows an overview of a hospital environment within an attacker trying to access the network by masquerade attacks as followings:

(t-1) The attacker tries to steal passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. Here (t-1) stands for "previously" or "earlier" before active attack, the attack may come from within hospital or outside.

(t-1, t, t+1) At any time (with a given frequency) the sensors devices regularly exchange message with data base where medical staff can find them.

(1-2) The medical staff are using their wireless sensor for logging into the server or data base through gateway.

(3) The attacker gets the victim's account ID and password for further privileges authentication.

(4-5) The attacker send a login request to the network using privileges of stolen ID and PW of the victim user.

(6-7) While the attacker has access to server, data base, and all network, he can now interact (pretending to be the legitimate member of the network) with either staff medical or sensors 'patients. Also, he can modify and delete patients 'records from the data base, make changes to network configuration and routing information.

IV. Proposed Middleware To Support Security in the e-Healthcare System

The proposed middleware secure approach is software based which can be implemented in a wireless or wired device. In this paper we consider a case where a user with his devices performs a mutual authentication process before accessing network and data. Before detailed discussion of the proposed scheme, some assumptions are made and are not supposed to be violated before mutual authentication starts.

- The user with his wireless devices has to register to the Network Administration in order to distribute the IDs, PW and Nonce in a secure manner.
- Registration and verification phase between user and wireless devices, Server and wireless devises are supposed to be honest without compromising each other. After registration phase is done, all components can start the mutual authentication process.

Figure 2 describes the proposed middleware security solution that is based mutual authentication before entering network and enjoying data. The following is the description of the protocol:

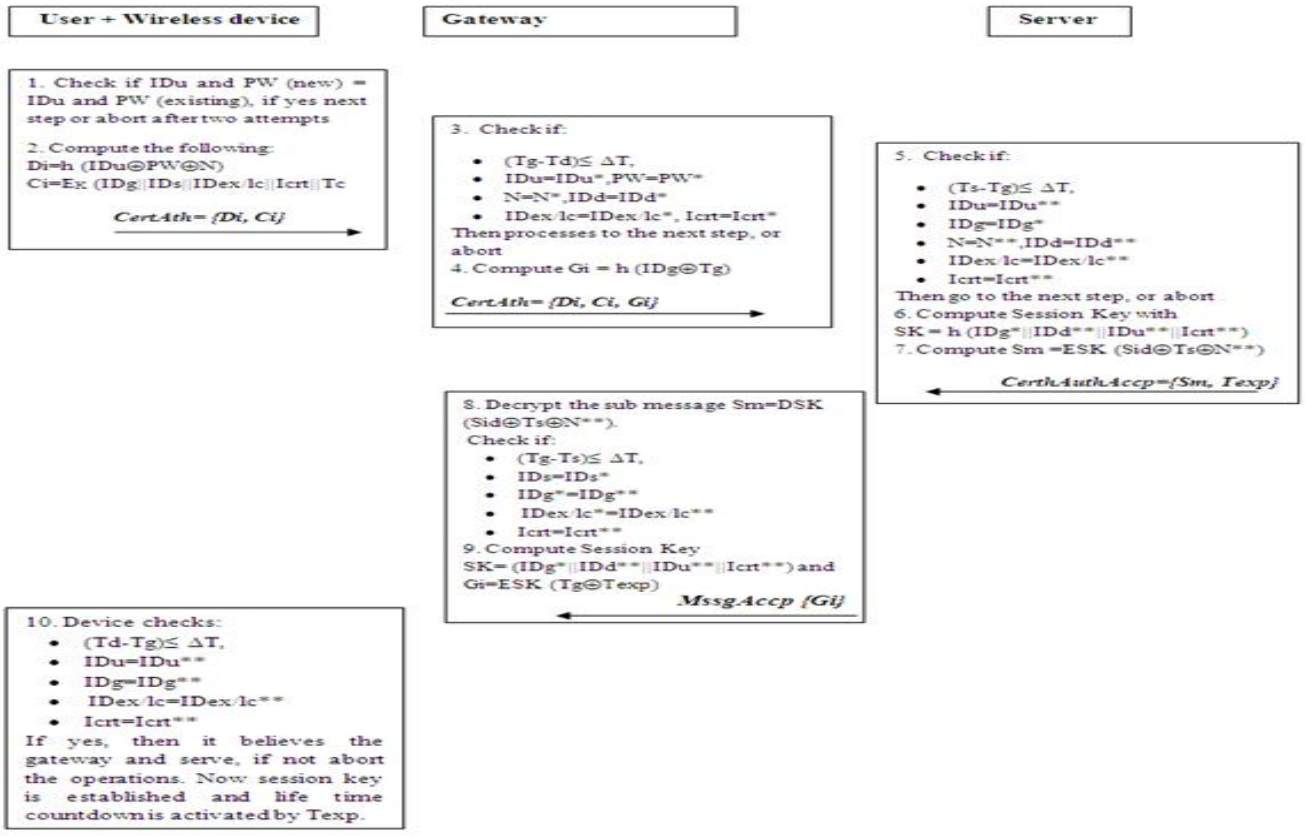

Figure 2. Proposed Middleware Solution besed Mutual Authentication

Step-1: The user sends an authentication login request with his IDu and PW to his device. The device system checks if the use requires the conditions pre-registered by verifying his ***"CertAuth"***. If yes the algorithm moves to the next step otherwise block the user if he attempts more than 2 times and then the user gets a message to indicated him that he is not allowed to access to device. The system recommends him to visit the Network Administrator.

Step-2: The wireless device sends now the request to the gateway for network accessibility. If the verification is true, then the gateway sends the message to the server to perform the other tasks of authentication. If not, the gateway returns back the message to device.

Step-3: While receiving the message from the gateway, sever performs mutual authentication by checking the content of the *CertAuth* and if everything is well then reply positively to gateway or abort the process and send back the message to gateway as well.

Step-4: Upon receiving the reply from server, the gateway perform the mutual authentication and check if it is the legitimate server, if yes the gateway send a message of acceptance with *MssAccp* to device in order to access both data and network, if not gateway will reject the message from server and will return back to him.

Step-5: When the device gets the acceptance message, it also performs the mutual authentication by checking different secrets parameters. If they are matching, then the session starts with session key and the countdown of the life time of the current session. This is the end the middleware security authorization identification.

V. SECURITY ANALYSIS

Masquerading user attack: The protocol is against this attack in its concept. Suppose an attacker steal the certificate, *CertAuth=<Di, Ci>*, he will try to login to the network but cannot pass the stolen certificate because the device system will check and will remark an attempt to re-use the certificate, then measure can be taken (i.e. unlock the device).

Masquerading gateway attack*:* Suppose that the attacker bypass security device, now the gateway will see that *Td, N* , and others *IDs* are already used, then measure can be taken (i.e.an alert can be generated to the server, and track process can start to localize the user device).

Mutual authentication*:* The proposed protocol provides the mutual authentication protocol for the whole communication process between all entities (*user, gateway and server).* This security feature is against known attack like compromised devices or replay and both they are sure that they are the legitimacies ones.

Session key establishment*:* A session key, *SK* is established between the communicating entities after authentication process. This key is different in each session and cannot be replayed after the session expires.

VI. CONCLUSIONS

This paper presented a middleware solution approach to support data and network security over e-Healthcare system sing medical sensor networks. It has been shown that a masquerade attack can be launched to the system and patients 'data are in danger. We proposed this middleware to counter this kind of attack where a user and all devices into the healthcare network are mutual authenticated. Finally a performance analysis has been done with regard to masquerade attack and the result reveals the efficient of the proposed solution

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. (Grant number: 2013-071188). And it also supported by the BB21 project of Busan Metropolitan City.

Bruce Ndibanje received the B.Sc degree in Computer Sciences, from Ngozi University, Burundi in 2006, the MS degree in Ubiquitous IT from Dongseo University in 2013. He has worked with many companies in the ICT domain such Huawei, United Nations, and Econet Wireless Burundi. Currently he is a Doctorate Researcher member of the Cryptography and Network Security Lab at Dongseo University, Busan, Korea since 2013. His research interest includes Wireless and Sensor Networks, Authentication Protocol, Security in: e-Healthcare System, Cloud Computing and Cellular Networks, Side-channel attack and Countermeasures. He is a member of the IEEE Computer Society.

Dr. Mangal Sain is an assistant professor in Department of Information Engineering at Dongseo University, Busan Republic of Korea. He received his Ph.D. majoring in Ubiquitous Information technology from Dongseo University, Busan, Korea in 2011. He finishes his master in 2003 from India His research interests are Wireless Sensor Networks, Ubiquitous Healthcare, Embedded Systems, Middleware, Cloud Computing and Cloud Middleware. He published more than 30 publications (Book Chapter, Journals, and Conference papers) in aforementioned areas. He is a member of IEEE and TIIS. His current research interests are in the fields of middleware, specially related with Cloud Computing.

Prof. Hoon Jae Lee He received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook national university in 1985, 1987 and 1998, respectively. He had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. He has published more than 250 papers and 50 patents. He has served as a reviewer for many international conferences and journals. His current research interests are in security communication system, side-channel attack, USN & RFID security. He is a member of the Korea institute of Information security and cryptology, IEEE Computer Society, IEEE Information Theory Society and etc.

REFERENCES

[1] Koch, S.; Hagglund, M. Health Informatics and the Delivery of Care to Older People. *Maturitas* **2009**, *63*, 195-199.

[2] Chung, W.Y.; Yan, C.; Shin, K. A Cell Phone Based Health Monitoring System with Self Analysis Processing Using Wireless Sensor Network Technology. In *Proceedings of 29th Annual International Conference on the IEEE EMBS*, Lyon, France, 23–26 August **2007**.

[3] Gravina, R.; Guerrieri, A.; Fortino, G.; Bellifemine, F. Giannantonio, R.; Sgroi, M. Development of Body Sensor Network Application Using SPINE. In *Proceedings of IEEE International Conference on Systems, Man and Cybernetics (SMC 2008)*, Singapore, 12–15 October **2008**.

[4] R. Sulaiman, D. Sharma, Ma Wanli, and D. Tran. "A Security Architecture for e-Health Services", in Advanced Communication Technology, 2008. ICACT **2008**. 10th International Conference on. 2008.

[5] D. R. Masys and D. B. Baker. "Patient-Centered Access to Secure Systems Online (PCASSO): A Secure Approach to Clinical Data Access Via the World Wide Web". **1997**.